State of Iowa Enterprise Mobile Device Security Standard

5-1-2008

Purpose

This policy establishes a consistent set of security practices for the use of mobile devices, such as the Blackberry and other smartphones, by state agencies and contractors.

Overview

Mobile devices combine telephone, email, text message, and web browsing functionality in a single wireless device. Mobile devices allow staff to keep current with agency activities while working away from the office. The decision of whether or not to allow the use of mobile devices by staff should be based on an assessment of the risks and business benefits of access. User requirements should be balanced against the risks associated with each of the mobile device functions under consideration. This standard provides a minimum set of security requirements for use of mobile devices.

Scope

This standard applies to mobile devices capable of sending and receiving email. This standard applies to all agencies as defined by Iowa Code Chapter 8A, Section 101. Non-participating agencies are encouraged to follow the guidelines in this and other enterprise level standards, as well as participate in enterprise level security programs.

Definitions

Selected terms used in the Mobile Device Standard are defined below:

- **Bluetooth** - Low power radio technology that allows devices to pair and connect wirelessly. Bluetooth-enabled devices can wirelessly connect to headsets and keyboards.
- **Desktop Redirector** – Software installed on a user's PC which allows the user to send and receive email on their mobile device while by-passing a central device server such as the BlackBerry Enterprise Server.
- **Peer-to-peer (also known as PIN-to-PIN)** - Messaging method which allows users to send unencrypted messages directly to other devices.
- **SMS (Short Message Service)** - A method of sending brief text messages of up to 160 characters between mobile phones; similar to a paging service.

Updates

This standard will be reviewed at least every two years and updated as needed.

ELEMENTS OF THE STANDARD

The following elements apply to all agency staff/contractors conducting state business on a mobile device.

1. Passwords/PINs: Passwords/PINs must be enabled for each device. Passwords/PINs must have a minimum length of 4 characters.
2. Erase Data and Disable Device: The device must have the ability to be remotely erased and disabled:
    a. After 10 unsuccessful password attempts.
    b. When reported lost or stolen.
3. Inactivity: The device must be set to lock after a minimum of 15 minutes of inactivity.
4. Emanations Security: The wireless functionality of devices must be disabled when in areas displaying, storing or transmitting confidential information.
5. Usage Policy: Agencies must:
    a. Have a policy covering the use of devices, and
    b. Ensure that staff receive and acknowledge the policy.
6. Training: Users are required to receive security awareness training covering use of mobile devices.
7. Short Message Service (SMS): Confidential information shall not be sent by SMS.
8. Peer to Peer Messaging (PIN to PIN): Confidential information shall not be sent by peer-to-peer messaging.
9. Security Patches: Software upgrades and security patches must be applied in a timely manner.
10. Personally Owned Devices: Personally owned devices connected to the enterprise email system:
    a. Must have the latest security patches installed in a timely manner.
    b. Are subject to all of the elements of this standard.
    c. Must be erased when the person leaves state government or the device is no longer used for state business.
11. Third Party Applications: Users may not download third-party applications to their device without prior approval.
12. Camera: Use of the camera feature is prohibited in areas displaying, storing or transmitting confidential information including health information.
13. Reporting: Users must report lost, stolen or missing devices to their agency, the Service Desk, and the Information Security Office. Notification shall take place as soon as possible, but no later than 24 hours, after the device is discovered to be missing.
14. Bluetooth: The following settings are required for devices using Bluetooth:
    a. Disable Discovery Mode,
    b. Pairing,
        i. Attempts to pair devices require prior management approval,
        ii. If prompted to pair with another Bluetooth device the user is to deny all requests and report such information to system administrators,
        iii. The Bluetooth functionality should be turned off unless a hands-free environment is required,
        iv. Data sent between paired devices must be encrypted.
15. Desktop Redirector: The BlackBerry Desktop Redirector may not be used.

Effective Date
This standard shall be effective July 31, 2008.

Enforcement
This standard will be enforced pursuant to Iowa Administrative Code 11—25.11(8A).

Variance
Iowa Administrative Code 11 - 25.11(2) provides for variances from security standards. Requests for a variance from any of the requirements of this policy will be submitted in writing to the Chief Information Security Officer prior to implementation.